

REMARKS

This communication is in response to the Final Office Action mailed July 12, 2004 in connection with the above-identified matter. Claims 14-26 remain pending in this application with claims 14 and 19 being the only independent claims. Claims 14 and 19 have been amended. No new matter has been added. Reconsideration of the outstanding rejections in view of the amendments to the claims and remarks presented below is respectfully requested.

On a formal note, the Examiner in the November 18, 2004 Advisory Action indicated that an initialed copy of the PTO Form 1449/SB08A of the references submitted with the Information Disclosure Statement filed simultaneously with the application was placed in the file. Applicant requests that the Examiner in the next communication provide a copy of the initialed form for applicant's records.

Claims 19-22 and 26 are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 5,883,960 (the '960 patent). Claims 14, 15, 23, 24 and 25 are rejected under 35 U.S.C. §103(a) as obvious over the '960 patent in view of U.S. Patent No. 5,557,679 (the '679 patent). Claims 16-18 are rejected under 35 U.S.C. §103(a) as obvious over the '960 patent and the '679 patent in view of U.S. Patent No. 5,793,866 (the '866 patent).

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Applicant submits that claim 19 is distinguishable over the '960 patent in that the claim recites "wherein at the manufacturer for pre-personalizing the chip a subscriber identification number (IMSI), a card number (ICCID) and an additional secret key Ki are stored". Thus, the claim expressly calls for all three parameters to be stored at the manufacturer of the chip. In the Final Office Action the Examiner referred to Col. 8, ll. 21-29 as teaching this limitation. Specifically, this passage discloses that public key KE_{COB} 44 may be written into ROM 34 in the

manufacturing process of the COB device 22 before it is shipped to the mobile unit manufacturer. The reference fails to disclose or suggest that the subscriber identification number (IMSI) and card number (ICCID) are also stored in the COB by the manufacturer, as claimed. Acknowledging the validity of this argument, the Examiner in his remarks in the Advisory Action now refers to another passage of the '960 reference, i.e., Col. 8, ll. 36-47, to teach this limitation. Specifically this second passage states "The EEPROM 36 can store personal identification such as MSN, MSI, etc., a carrier public key KE_{Cj} 50 corresponding to a carrier secret key KD_{Cj} known only to the communications carrier, and a mobile unit public key KE_{MSNi} 52 corresponding to a mobile unit secret key KD_{MSNi} known only to the manufacturer of the mobile unit." Applicant disagrees with the Examiner's position that this text reads on the claimed limitation. ROM 34 (referred to in Col. 8, ll. 21-29) is a different memory device from the EEPROM 36 (described in Col. 8, ll. 36-47). Only writing of the KE_{COB} 44 into ROM 34 is expressly disclosed in the '960 patent as occurring in the manufacturing process of the COB device 22. In contrast, the storage of parameters (e.g., MSN, MSI) in the EEPROM 36 is not disclosed as occurring during manufacturing of the COB, as expressly called for in claim 19. To the contrary, the reference only discloses that the carrier public key KE_{Cj} 50 is written into the EEPROM 36 in the manufacturing process of the mobile unit (Col. 8, ll. 48-50). Absent an express teaching or suggestion in the '960 reference, it is improper for the Examiner to infer that the subscriber identification number (IMSI) and card number (ICCID) are stored during the manufacturing process of the COB.

The next distinguishing feature of claim 19 over the prior art is the limitation "wherein the chip itself derives an initial secret key Ki_1 from the secret key Ki which is known and entered into the chip". Specifically, the Examiner in the Advisory Action in maintaining his prior art rejection states:

"The office disagrees reference '960 shows how the chip itself or COB derives the an initial secret key Ki_1 in col. 13, line 40 through col. 14 line 29. The COB device generates a random number, which is sent to the controller as well as stored into RAM. Then a registration start request is initiated the carrier returns a secret key which is sent to the controller of the mobile unit, the mobile unit then sends this secret key to the COB which compares

the secret key with random value to see if they match, if a match is obtained then the KE_{CN} is returned to the controller. The act of generating a random number and comparing the secret key with the integer value and the public key is the same as deriving a secret key.”

Applicant once again respectfully disagrees with the Examiner’s position that these steps of the ‘960 patent are analogous to the claimed limitation. Referring to claim 19, the limitation in question expressly states “the chip itself derives an initial secret key Ki_1 from the secret key Ki which is known and entered into the chip” during manufacture as expressed in the preamble (emphasis added). The text of the ‘960 patent in Col. 13, line 40 through col. 14, line 29 cited by the Examiner provides that the COB device generates a random number. In order for the patented invention to read on the limitation in question, the random number would have to be generated from the secret key stored by the manufacturer in the COB, as claimed. The random number is generated in the COB, but is not disclosed as being derived from the secret key of the COB that is known and written during manufacturer of the chip, as called for in the preamble and body of claim 19.

The last limitation in question in claim 19 refers to “the chip (COB) being Tool-kit enabled and includes means for communication with a security center (SC) and negotiating a new secret key Ki_2 ”. In the Advisory Action the Examiner states “The office disagrees the claimed invention indicates that the ‘wherein the chip in the terminal equipment is Toolkit-enabled’ the terminal equipment has the same meaning as the ‘controller of the mobile unit’ like the terminal the controller of the mobile unit has a component for communicating with the security center (or carrier’s terminal) ‘960 shows the negotiation of the secret key as shown above.” Despite the Examiner’s conclusory statements he has failed to expressly point out where the ‘960 reference teaches that the COB is Tool-kit enabled. No such reference is found anywhere in the ‘960 reference. As for the limitation that the COB includes means for negotiating a new secret key, the Examiner relies on his remarks with respect to the limitation discussed in the preceding paragraph. Applicant refers the Examiner to the arguments above as to why the limitation that “the chip itself derives an initial secret key Ki_1 from the secret key Ki which is known and entered into the chip” is not taught by the ‘960 reference.

Furthermore, applicant questions why the Examiner grouped together the previously discussed limitation and the present limitation in question when in fact they differ in scope. The present

limitation in question relates to deriving a new secret key Ki_2 distinguishable from the initial secret key Ki_1 found in the previous paragraph and limitation. Thus, the '960 patent fails to disclose or suggest that the COB has means for negotiating either an initial secret key or a new secret key, as found in claim 19.

The other independent claim, that is claim 14, is rejected as obvious over the '960 patent in view of the '679 patent. The preamble states, "wherein at the manufacturer for pre-personalizing the chip a subscriber identification number (IMSI), a card number (ICCID) and an additional secret key Ki are stored". This passage is patentable over the prior art reference for the same reasons provide above with respect to independent claim 19 wherein the Examiner referred to the same passage of the prior art reference for teaching the claimed limitation.

Limitation b) in the body of claim 14 states "obtaining the (ICCID) card number and the (IMSI) subscriber identification number from a number pool, the chip itself derives an initial secret key Ki_1 from the secret key Ki which is known and entered into the chip". Applicant for the reasons stated above has distinguished with respect to claim 19 why the '960 patent fails to teach "the chip itself derives an initial secret key Ki_1 from the secret key Ki which is known and entered into the chip". Therefore, limitation b) of claim 14 having similar language is patentable over the art of record for the same reasons.

Applicant next distinguishes the next four limitations of claim 14 over the prior art. Limitations c)-f), states "c) making an entry in an authentication center (ACF) and a home location register (HLR) as soon as the subscriber has entered into a contract with a network operator; d) deriving at the authentication center (AC) the initial secret key Ki_1; e) setting the conditions of the network so that during logon to the network a connection is established from the chip to the security center (SC) of the network operator; f) routing the connection from the chip to the security center (SC) during the first logon". In the Advisory Action the Examiner refers to the '960 patent as including a "carrier terminal" and "dealer number". Furthermore, the Examiner points out in Col. 21, ll. 6-7 that "Registration with any additional communications carrier is performed in the same sequence." In summary, the Examiner has merely asserted that the "carrier terminal" is analogous to the claimed "security center" and presumably that the "dealer number" is equivalent to the authentication center. The Examiner fails to specifically

point out a teaching in the reference for each feature in claim 14, namely, (i) the making of an entry in an authentication center (ACF) and a home location register (HLR) as soon as the subscriber has entered into a contract with a network operator; ii) deriving at the authentication center (AC) the initial secret key Ki_1 ; iii) that conditions of the network are set so that during logon to the network a connection is established from the chip to the security center (SC) of the network operator; and iv) routing the connection from the chip to the security center (SC) during the first logon. Absent such specific teaching in the reference for each limitation, applicant submits that the Examiner has failed to set forth a proper basis for anticipation of the claimed invention.

As for the limitation g) of “negotiating between the chip and the security center (SC) a new second secret key Ki_2 for the chip” (emphasis added) in claim 19, the Examiner asserts that col. 23, ll. 45-67 discloses a sequence for updating the keys. Applicant respectfully disagrees with the Examiner that this reference reads on the claimed limitation. The passage referred to by the Examiner discusses a sequence for updating the “personal information” assigned to the subscriber when an IC card is broken and replacement is requested. The purpose or goal of the updating sequence is to prevent the duplication of a legally registered IC card. Figs. 36 to 38 are diagrams showing the first, middle, and last portions of the processing sequence for updating IC card’s personal information none of which disclose updating the secret key KE_{COB} for the chip, as claimed. The patent fails to expressly mention the secret key for the chip, disclosing only that personal information may include “MSN, MSI, etc., a carrier public key KE_{Cj} 50 corresponding to a carrier secret key KD_{Cj} known only to the communications carrier, and a mobile unit public key KE_{MSNi} 52 corresponding to a mobile unit secret key KD_{MSNi} known only to the manufacturer of the mobile unit” (Col. 8, ll. 36-41). Instead, the ‘960 patent teaches away from the present claimed invention in expressly stating that the secret key KE_{COB} for the chip is stored in an unalterable ROM and thus is not a parameter to be updated (Col. 12, ll. 23-24).

In addition, claim 14, as amended, which now reads “unconditionally disabling the conditions of step e)” is further distinguishable over the ‘960 patent. To reiterate, the condition set forth in step e) that is to be disabled includes “setting the conditions of the network so that during logon to the network a connection is established from the chip to the security center (SC)

of the network operator”. The reason in step h) for disabling the conditions of step e) is that this operation need only performed once. The Examiner in his remarks in the Advisory Action states “The Office disagrees the NG display means that the mobile device cannot be used with the communication network. The predetermined limit is the amount of times the mobile device can attempt to use the communication network, when the limit is reached the mobile device is disabled, see ‘960 col. 14, lines 1-14.” Applicant disagrees slightly with the Examiner’s interpretation of the relevant passage of the ‘960 reference and summarizes the passage herein for clarification. The reference discloses that the IC card stores information that restricts its use only to the mobile units approved by the communication carrier for connection. Different carrier public keys KE_{CN} are stored in the EEPROM at different positions specified by the integer J. A determination is made whether the decrypted results $E(KD_{CN}, RDM)$ matches the RDM contained in the entered command associated with integer J. If not, then a comparison is made with the next carrier public key KE_{CN} stored at the next incremented position (J+1). This process is repeated until a match is identified or otherwise a predetermined integer I is reached representing the total number of carrier public keys stored whereby NG is displayed. The present claimed disabling step is distinguishable over the prior art in that it is not conditional. The reason being that the operation in step 3) need only performed once. In contrast, the ‘960 patent refers to a conditional limit that must be satisfied before the mobile unit is classified as not usable.

Applicant submits that dependent claims 15, 20, 21, 24 and 26 are further distinguishable over the ‘960 patent. Specifically, claim 15 states “wherein the initial secret key Ki_1 which is first stored in the chip, is not transmitted to and stored in the authentication center (AC) before the contract is established”; claim 20 states “wherein the chip includes means for receiving data from the security center (SC) and means for writing the received data to the memory”; claim 21 states “wherein the chip comprises a microprocessor for negotiating a secret key with the security center (SC)”; claim 24 states “wherein step g) further comprises negotiating at the security center (SC) the PUK with the chip or generated in the security center (SC) and transmitted to the chip”; claim 26 states “wherein the chip includes means for reading data received from the security center (SC) in memory, modifying the data and transmitting the data



to the security center (SC)". The prior art fails to mention these specific limitations recited in the claims in question.

For the foregoing reasons applicant submits that independent claims 14 and 19 are patentable over the prior art of record. The remaining claims depend from one of these independent claims and thus are also patentable over the art of record. Applicant submits that the application is in condition for allowance and passage to issuance is respectfully requested.

If any additional fees are required, authorization is hereby provided to charge our U.S. Patent and Trademark Deposit Account No. 14-1263.

Respectfully submitted,

Christa Hildebrand
Reg. No. 34,953
Attorney for Applicant

Norris McLaughlin & Marcus P.C.
875 Third Avenue, 18th Floor
New York, N.Y. 10017
Telephone: (212)808-0700
Facsimile: (212)808-0844